IN THE CLAIMS

Please amend Claims 1-6, 8-17, and 19-26 as indicated.

1. (Currently Amended) A method for providing automated tracking of security vulnerabilities, comprising:

~~performing~~ using a computing device to perform a security vulnerability assessment on a system;

storing data obtained from the security vulnerability assessment in a security vulnerability database;

determining, using a computer program, a security vulnerability score based on a plurality of security vulnerability factors identified by the security vulnerability assessment; and

determining a time to fix a security vulnerability identified by the security vulnerability assessment of the system based on the determined security vulnerability score.

2. (Currently Amended) The method of claim 1, wherein determining the security vulnerability factor further comprises considering the frequency the identified security vulnerability occurs in the system.

3. (Currently Amended) The method of claim 2, wherein determining the security vulnerability factor further comprises the criticality of an element in the system presenting the security vulnerability and a rating of the severity of the security vulnerability.

4. (Currently Amended) The method of claim 1 further comprising determining an IP address associated with the security vulnerability.

5. (Currently Amended) The method of claim 4 further comprising entering the IP address and a description of the identified security vulnerability in a tracking database.

6. (Currently Amended) The method of claim 1 further comprising determining delinquent security vulnerabilities based upon the determined time to fix the security vulnerability identified by the security vulnerability assessment.

7. (Original) The method of claim 6 further comprising providing notification of determined delinquencies.

8. (Currently Amended) The method of claim 6 further comprising re-running a scan profile when notification is received that the security vulnerability has been fixed.

9. (Currently Amended) The method of claim 8 further comprising determining whether the security vulnerability still exists and archiving records associated with the security vulnerability when the security vulnerability does not still exist.

10. (Currently Amended) A method for determining a criticality factor for a security vulnerability in a computer system, comprising:

entering in a database security vulnerabilities identified during a security vulnerability assessment;

monitoring a frequency of occurrence for the identified security vulnerabilities; and

assigning a security vulnerability factor to a security vulnerability based upon the frequency of occurrence of the security vulnerability in the system.

11. (Currently Amended) The method of claim 10, wherein the assigning a security vulnerability factor further comprises considering a criticality of an element in the system presenting the security vulnerability and a rating of the severity of the security vulnerability within the system.

12. (Currently Amended) An apparatus for providing automated tracking of security vulnerabilities, comprising:

a memory for storing program instructions; and

a processor, configured according to the program instructions for performing a security vulnerability assessment on a system, storing data obtained from the security vulnerability assessment in a security vulnerability database, determining a security vulnerability score based on a plurality of security vulnerability factors identified by the security vulnerability assessment and determining a time to fix a security vulnerability identified by the security vulnerability assessment of the system based on the determined security vulnerability score.

13. (Currently Amended) The apparatus of claim 12, wherein the processor considers a frequency of the identified security vulnerability in the system when determining the security vulnerability factor.

14. (Currently Amended) The apparatus of claim 13, wherein the processor further considers the criticality of an element in the system presenting the security vulnerability and a rating of the severity of the security vulnerability when determining the security vulnerability factor.

15. (Currently Amended) The apparatus of claim 12, wherein the processor determines an IP address associated with the security vulnerability.

16. (Currently Amended) The apparatus of claim 15, wherein the processor enters the IP address and a description of the identified security vulnerability in a tracking database.

17. (Currently Amended) The apparatus of claim 12, wherein the processor identifies delinquent security vulnerabilities based upon the determined time to fix the security vulnerability identified by the security vulnerability assessment.

18. (Original) The apparatus of claim 17, wherein the processor provides notification of the identified delinquencies.

19. (Currently Amended) The apparatus of claim 17, wherein the processor re-runs a scan profile when notification is received that the security vulnerability has been fixed.

20. (Currently Amended) The apparatus of claim 19, wherein the processor determines whether the security vulnerability still exists and archives records associated with the security vulnerability when the security vulnerability does not still exist.

21. (Currently Amended) An apparatus for determining a criticality factor for a security vulnerability in a computer system, comprising:

a memory for storing program instructions; and

a processor, configured according to the program instructions for entering in a database security vulnerabilities identified during a security vulnerability assessment, monitoring a frequency of occurrence for the identified security vulnerabilities and assigning a security vulnerability factor to a security vulnerability based upon the frequency of occurrence of the security vulnerability in the system.

22. (Currently Amended) The apparatus of claim 21, wherein the processor considers a criticality of an element in the system presenting the security vulnerability and a rating of the severity of the security vulnerability within the system when assigning a security vulnerability factor.

23. (Currently Amended) An apparatus for providing automated tracking of security vulnerabilities, comprising:

means for storing program instructions; and

means configured according to the program instructions provided by the means for storing for performing a security vulnerability assessment on a system, storing data obtained from the security vulnerability assessment in a security vulnerability database, determining a security vulnerability score based on a plurality of security vulnerability factors identified by the security vulnerability assessment and determining a time to fix a security vulnerability identified

by the security vulnerability assessment of the system based on the determined security vulnerability score.

24. (Currently Amended) An apparatus for determining a criticality factor for a security vulnerability in a computer system, comprising:

means for storing program instructions; and

means configured according to the program instructions provided by the means for storing for entering in a database security vulnerabilities identified during a security vulnerability assessment, monitoring a frequency of occurrence for the identified security vulnerabilities and assigning a security vulnerability factor to a security vulnerability based upon the frequency of occurrence of the security vulnerability in the system.

25. (Currently Amended) A program storage device readable by a computer, the program storage device tangibly embodying one or more programs of instructions executable by the computer to perform a method for providing automated tracking of security vulnerabilities, the method comprising:

performing a security vulnerability assessment on a system;

storing data obtained from the security vulnerability assessment in a vulnerability database;

determining a security vulnerability score based on a plurality of security vulnerability factors identified by the security vulnerability assessment; and

determining a time to fix a security vulnerability identified by the security vulnerability assessment of the system based on the determined security vulnerability score.

26. (Currently Amended) A program storage device readable by a computer, the program storage device tangibly embodying one or more programs of instructions executable by the computer to perform a method for determining a criticality factor for a security vulnerability in a computer system, the method comprising:

entering in a database security vulnerabilities identified during a security vulnerability assessment;

monitoring a frequency of occurrence for the identified security vulnerabilities; and

assigning a security vulnerability factor to a security vulnerability based upon the frequency of occurrence of the security vulnerability in the system.